AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

19820 Oak River Dr, Petersburg, Virginia 23802

Case No. 3:20SW035

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

located in the EASTERN District of VIRGINIA, there is now concealed *(identify the person or describe the property to be seized)*:

9820 Oak River Dr, Petersburg, Virginia, is a one story single family home with a possible basement. The front door is red with beige in color paneling. The house has red shutters and wood steps going up to the front door.
See Attachment B of the attached Affidavit, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2422(b), 2252A, 2251	Coercion and Enticement, Possession, Receipt and Distribution of Child Pornography, Sexual Exploitation of Children

The application is based on these facts:

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Christopher Ford Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 2/12/2020

City and state: Richmond, VA

/s/

Judge's signature

Roderick C. Young
United States Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Richmond Division

IN THE MATTER OF THE SEARCH OF 19820 OAK RIVER DR, PETERSBURG, VA 23802.

. No. 3:20SW035

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Christopher A. Ford, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

I make this affidavit in support of an application for a search warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure to search the premises known as 19820 Oak River Dr., Petersburg VA 23802 (referred to hereinafter as "SUBJECT PREMISES"), further described in Attachment A, for the property described in Attachment B.

1. Your Affiant has been employed by the FBI since May 2016, and I am currently assigned to the FBI Washington Field Office Child Exploitation and Human Trafficking Taskforce. While employed by the FBI, I have investigated federal criminal violations related to cyber national security crime, violent crime, high technology or cyber-crime, missing persons, and child exploitation, including child pornography offenses. I have received training in the area of child pornography and child exploitation. Additionally, I have investigated and assisted in the investigation of criminal matters involving: the sex trafficking of children, in violation of Title 18 United States Code, Section 1591; the sexual exploitation of children, in violation of Title 18, United States Code, Sections 2251, 2252, 2252A, and 2422. Moreover, I am a federal law enforcement officer authorized by the Attorney General to enforce violations of the laws of the United States including but not limited to, Title 18, United States Code, Sections 1591, 2251,

2252, 2252A, 2422 and 2423. Prior to this assignment, I worked as Consultant for Booz Allen Hamilton and Deloitte, specializing in software development and software engineering. I have a Bachelors of Science and a Masters of Science in Information Technology.

2. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. The facts as set forth in this affidavit establish that there is probable cause to believe that violations of 18 U.S.C. §2422(b), Coercion and Enticement; 18 U.S.C. §2251, Sexual Exploitation of Children; and 18 U.S.C. § 2252A, Receipt and Distribution of Child Pornography, occurred and that a search of the SUBJECT PREMISES described in Attachment A will yield evidence, contraband, or fruits of these crimes, as described in Attachment B.

JURISDICTIONAL AUTHORITY

4. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction," as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

RELEVANT STATUTORY PROVISIONS

5. **Coercion and enticement**: 18 U.S.C §2422(b) provides that it is a crime for one, using the mail or any facility or means of interstate or foreign commerce, to persuade, induce, entice, or coerce any individual who has not attained the age of 18 years, to engage in any sexual activity for which any person can be charged with a criminal offense.

6. **Sexual Exploitation of Children**: 18 U.S.C §2251 provides that it is a crime for one using the mail or any facility or means of interstate or foreign commerce, to persuade, induce, entice, or coerce any individual who has not attained the age of 18 years, to engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct.

7. **Receipt and Distribution of Child Pornography:** 18 U.S.C. § 2252A, provides that it is a crime for one to receive or distribute child pornography, using the mail or any facility or means of interstate or foreign commerce.

8. **Child pornography** means any visual depiction, in any format, of sexually explicit conduct where: (A) the production involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital or computer-generated image that is substantially indistinguishable from that of a minor engaged in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexual explicit conduct. *See* 18 U.S.C. § 2256(8).

9. **Visual depictions** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which are capable of conversion into a visual image, and data which are capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. See 18 U.S.C. § 2256(5).

10. **Minor** means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

11. **Sexually explicit conduct** means actual or simulated: (i) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or

opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2)

12. **Interstate Communications:** 18 U.S.C §875(d) provides that it is a crime for one, with intent to extort from any person,, any money or other thing of value, to transmit in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime.

TECHNICAL TERMS

Based on my training and experience, I use the following technical terms to convey the following meanings:

13. **Cellular telephone**: A cellular telephone (or mobile telephone, or wireless telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

14. **Internet**: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

15. **Computer hardware**" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

16. **Internet Protocol ("IP") Address** is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 149.101.1.32). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

17. **"Internet Service Providers,"** or "ISPs," are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other

communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line ("DSL"), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

PROBABLE CAUSE

18. Beginning on February 13, 2019, the FBI met with a Complainant[1] on multiple occasions. The Complainant informed the FBI of the following:

19. On or about December 2015, Joshua Brady hereinafter referred to as ('Brady'), contacted the Complainant via EpikChat[2] when she was 14 years-old. Brady told the Complainant that his name was Joshua Weston. Brady claimed to be a member of the prominent Weston family from the United Kingdom and Canada, and told the Complainant that he would kill her if she did not listen to him. During one conversation, Brady told the Complainant that he was once so upset with a family that he hired an assassin to murder them. Brady faked a British accent to convince the Complainant that he was in fact British.

---

[1] The Complainant's name is known to law enforcement. It is being withheld for the purposes of this affidavit to protect the victim's safety and privacy.

[2] EpikChat is an online video chat community where users can connect with one another and communicate in chat rooms.

20. Between approximately December 2015 and July 2016, when the Complainant was 14 and 15 years-old, the Complainant and Brady communicated via telephone, text message, Skype (video chat) and various other social media platforms such as Snapchat, Facebook and Instagram. The video chats between the Complainant and Brady were mostly sexual in nature. During these video chats, the Complainant would undress, causing her bare breasts and genitals to be visible to the camera. The video chats typically occurred on a nightly basis. During the video chats on Skype, Brady would force the Complainant to perform various sexual acts, to include piercing her nipples and labia with safety pins and masturbation, among other things, as "punishments". Punishments became a nightly thing and progressed overtime. On one occasion, he instructed her to insert the handle of a plunger into her vagina as he watched on Skype. It was common for him to send her pictures of herself from the punishment sessions. Brady threatened to tell her family if she did not do everything he asked of her, even threatening to kill them if she did not obey.

21. Brady instructed the Complainant to send pictures of her nude breasts and vagina to him on several occasions. On one occasion, Brady instructed the Complainant not to wear underwear to school, to take pictures of her vagina, and then send the pictures to him while she was at school. The Complainant subsequently sent the pictures that Brady requested via text message.

22. On or about November 2019, Brady initiated contact with the Complainant via Snapchat direct message, utilizing usernames "Boris Kazinkovich" and "TheRealBoris7". Using Snapchat, Brady told her that she was being accused of sexual harassment. On or around December 17, 2019, Brady sent the Complainant's father a text message with a picture of the Complainant in a bikini. The Complainant was about 15 or 16 years-old at the time the photo was

taken, and she believes that Brady got the photo from one of her public social media accounts. In the text message to the Complainant's father, Brady asked if he knew what his daughter was doing right now. The Complainant's father directed Brady not to contact him again.

23. On or about December 18, 2019, Brady and the Complainant communicated via Snapchat direct message for several hours. During the conversation, Brady told the Complainant that his real name was Burnett, not Weston. Brady also apologized to the Complainant for sexually exploiting her when she was a minor, specifically the body piercings and plunger incident.

24. Brady stated that he shared an account with two other men, and that they used the account to "troll people" online. Brady admitted to taking pictures and videos of the Complainant during the Skype video chat calls while the Complainant was a minor, and engaging in the sex acts noted above. Brady also admitted to sending the Complainant pictures of his penis, which he referred to as "dick pics," when she was under the age of 18.

25. Brady further told the Complainant that he had previously seen her in person as a minor when she "walked past him several times" in the vicinity of Neiman Marcus in Mazza Gallerie in the Washington, DC area.

26. On or about December 18, 2019, the Complainant exchanged the following chats with Brady (The Complainant's account has a display name of "Corimem," while Brady's display name on Snapchat is "Boris Kazinkovich (Boris)"):

Corimem: Oh did you record me I always wondered that
Boris: Actually you want me to be honest?
Corimem: Yes no please lie to me
Boris: Okay no never ever
Corimem: That's a lie come on
Boris: You told me to lie
Corimem: Oh so yes you did?

Boris: I recorded you at the beginning and showed/told you. You knew that the other times I told you it was a lie. I never had a recording and actually by the time school was out
Corimem: You sent me pictures of myself
Boris: I had no recordings
Corimem: At some points
Boris: Yeah that's not a recording
Corimem: Ok so pictures
Boris: Like I took pictures sometimes yeah but after you were out in June none deleted them wiped that computer even told my dad first he made me tell my mom who made me go to tell my grandma. Which was the hardest part tbh.

As the chat continued, Brady and the Complainant exchanged the following messages:

Boris: If I kept it online it wasn't real even though it was? You know?
Corimem: Yes I know
Boris: So I really honestly wish I had just been smarter and been honest
Corimem: Yeah I still talk to people I met online when was lole like 13/14 only one but yeah you tell the truth
Boris: If we were to meet where would it even be
Corimem: Starbucks
Boris: [emoji] basic white girl at her finest

During the chat, Brady attempted to apologize to the Complainant for his actions:

Boris: I'm sorry don't ever feel like you're really anything less than special. Even as bad as I was and as bad as I behaved you really did light up my day
Corimem: I'm glad I could entertain.
Boris: Not like that I mean I really cared "Complainant's name" you really were amazing
Corimem: I know I don't know why you think that you didn't know me
Boris: Yes I did
Corimem: You knew my fear
Boris: Nah

Brady then made statements indicating he knew the Complainant was a minor when he first began chatting with her using various websites and social media applications:

Corimem: You really cared for me through all the lies
Boris: Yes I really did
Corimem: I was so fucking stupid
Boris: I really loved you ("Complainant's name") And so was I stupidity is part of growing up
Corimem: I still am
Boris: Eh

Corimem: Don't get me wrong
Boris: You will be alright you're a baby engineer after all
Corimem: Yeah that on the honor roll wooo
Boris: One of my friends I went to school with is doing his PhD in Sociology there he's the one who told and "Complainant's name"we call it deans list silly
Corimem: Whatever
Boris: You're out of high school now
Corimem: I don't know it was on my transcript
Boris: Yeah wait high school?
Corimem: No
Boris: Or Purdue? Ah yeah deans list having honors
Corimem: Hell no I did poorly in school High school
Boris: I ruined that
Corimem: You didn't help
Boris: Sorry
Corimem: My freshmen year was a disaster
Boris: Yeah I imagine
Corimem: Sophomore yeah wasn't great Junior and senior year I pulled myself together
Boris: Good do you have any other questions?
Corimem: None that I can think of I'm like Spinning

Brady admitted that he had told other people what he had done to the Complainant:

Boris: Well that's good I told a few more than that
Corimem: You told people
Boris: Yes
Corimem: And they were just like ok with it
Boris: Depends on who for their reaction my parents were pissed and disappointed even though they were not together it's why I went to the hospital
Corimem: I'm sure you didn't mention all of it though
Boris: Oh I told my dad literally everything
Corimem: The safety pins
Boris: The plunger yep all of it threats to Kate I didn't leave anything out had to be honest to move forward
Corimem: He wasn't mike like hey go to the police and turn yourself in?
Boris: Oh my dad was royally pissed no but he didn't speak to me for a bit

During this same exchange, the Complainant confronted Brady about gifts that he had sent her father:

Corimem: Why did you send my father that basket that scared the shit out of him and me
Boris: Because I liked you? Yeahhh didn't mean to scare him
Corimem: The fuck part of me telling you

Boris: I developed feelings and knew I was gonna have to meet him
Corimem: No don't do that
Boris: Right Idk showing off impressing you sorta liking you
Corimem: I thought you were going to kill me
Boris: Building up the story seriously? Why?

27. Records provided pursuant an administrative subpoena to Snapchat revealed that between approximately December 12, 2019, and January 1, 2020, the IP address used to access "TheRealBoris7" was 2601:5cb:4100:4d60:4053:2b62:d3a:543a. The account appeared to be created on October 30, 2019.

28. A search of publicly available sources indicated the Internet Service Provider (ISP) who owned IP address 2601:5cb:4100:4d60:4053:2b62:d3a:543a during that time is Comcast. According to administrative subpoena results from Comcast, the subscriber to IP address 2601:5cb:4100:4d60:4053:2b62:d3a:543a was Dana Hart with the SUBJECT PREMISES as the associated address. Dana Hart is Brady's mother.

29. On or about December 19, 2019, a preservation request was submitted to Snapchat for all content associated with username "TheRealBoris7".

30. In January of 2013, Brady was convicted in federal court of Forgery of a Judge's Signature, in violation of 18 U.S.C. §505. Law enforcement has also investigated Brady for complaints that he victimized multiple underage females, and adults, since at least 2012. Additionally, law enforcement investigations identified Brady as a suspect where he allegedly impersonated a Defense Intelligence Agency official in order to recruit people to rob banks in the Northern Virginia area. Brady has also been identified in state investigations using the persona "Joshua Weston" to target women for abuse.

31. On January 10, 2020, a recorded control call between the Complainant and Brady took place at the Complainant's residence in Washington, DC. The call took place via Snapchat, and the Complainant verified that Brady used the username, "TheRealBoris7", which is the same account subpoenaed above, to conduct the call. The following are pertinent statements made by, or acknowledged by Brady regarding his abuse of the Complainant. There are times within the call that a topic is covered multiple times. The statements are in chronological order:

Regarding trolling and a fake British accent:

Brady: [unclear transmission] I'm just a troll right now
The Complainant: Is that what you do best?
Brady: I do troll
Brady: I do voices
The Complainant: Really I couldn't tell. When you for six months straight put on a British accent.
[Brady does some sort of voice]
The Complainant: I hate this so much
Brady: I know how to do a British accent though
The Complainant: Yeah I know that that would make me freak out, it doesn't matter how long ago it was. It still hurts my soul a little bit.
Brady: I did it for more than six months…I regularly used the accent beyond that.
The Complainant: For what
Brady: I still use the accent. Just not nearly as often.

Regarding how long the Complainant and Brady have been in contact the following was said:

The Complainant: This is so strange
Brady: What's strange?
The Complainant: I don't know…this…it's our four year anniversary
Brady: Oh/No shit!
The Complainant: I know right…or five…wait how does time work
Brady: Four..four
The Complainant: Four...even though I'm 19.
Brady: Correct you were 15 at the time….take away four years…yeah
The Complainant: Oh yeah no doubt cause freshman year to freshman year

Brady describes how he identified and targeted the Complainant:

The Complainant: I remember the first message you sent

Brady: EpikChat...yes
The Complainant: The first message you sent was, hello...its me like the stupid Adele song.
Brady: That was my username
The Complainant: But that was the message you sent me on my phone...like the first text, I remember that.
Brady: mmhmmm
The Complainant: What else do I remember
Brady: Okay, well your username on there was called [unclear] and you had a Kik that you provided [unclear] and you would also give it to other people. Your Kik name happens to also be the name you used for your uh...naughty stuff.
The Complainant: Oh I didn't know that I had you on that one.
Brady: It's me...Oh I had that one originally and then the actual, your original, like real one.
The Complainant: My real what?
Brady: Where you had like friends, your real Kik.
The Complainant: Oh yeah
Brady: Mmmhmm….and that is where I had enough to identify who you were and tie in your parents by using the last name and the general area and doing some other little computer things and BING there we go, we know this is her.
The Complainant: That's terrifying
Brady: And I got your parents information from a catholic church website. Where they were both listed as points of contact for a [unclear] program ah for like parishioners in need, they needed something and go from there. And I went to the DC bar and I got your mom's info and it just spiraled from therefore.
The Complainant: But like I also told you a bunch stuff too stupidly.
Brady: I...had, once I had the ability to identify who you were, everything you told me just validated the direction I went in with things. I'm really good like skip tracing people
The Complainant: Skip tracing?
Brady: Yeah like finding people who don't want to be found
The Complainant: Can you find yourself?
Brady: I can actually thats how I make shit disappear

Brady used his British accent during the next segment. The Complainant told Brady how the accent disturbs her and brings back memories of the time of abuse:

The Complainant: Yeah you came back four years later
Brady: It's okay this time I'm not going to hurt ya
The Complainant: Thanks
Brady: Mmmhhmmm...I really didn't like hurting you before.
The Complainant: Then why did you do it?
Brady: [unclear] It started off like I told you, trolling you, internet lulls, and it evolved and went from there to a bunch of just other crud where I didn't really have control. I wasn't driving the situation, responsible for it.

Brady and the Complaint discuss pictures that he saved from the time of abuse:

Brady: I have way too many pictures
The Complainant: And you said you deleted all of the ones of me?
Brady: Wow...thats kind of crazy
The Complainant: Hm?...what
Brady: Looking through some of these pictures
The Complainant: What are they of?
Brady: Just from earlier this year, and earlier in the school year I should say.
The Complainant: Ah.

Brady: Save them I don't care...what are you going to do with them?
The Complainant: These don't really matter to me, they're not of me.
Brady: You want to see pictures of you? Here. I will show you pictures of you.
The Complainant: You still have pictures of me saved?
Brady: I do.
The Complainant: Thought you said you deleted them all.
Brady: No. [unclear] bad pictures of you.
The Complainant: Ah.
Brady: I'll have to get to that later, but I will send some to you. Maybe it will jog your memory.

The Complainant then talks about the incident with the plunger:

The Complainant: I was really hoping I could find that…
Brady: [Interrupts but is unclear]
The Complainant: Hm?
Brady: Really hope what?
The Complainant: I was really hoping I could find that one picture on my laptop that the other number sent to me.
Brady: What other number sent to you?
The Complainant: A while back, remember when we were talking and another number sent me back the picture of me with the handle, in my vagina, remember?
Brady: The handle?
The Complainant: Of the plunger.
Brady: Someone sent that to you?
The Complainant: Well no you did I think right? Didn't you?
Brady: Not for the plunger, no. Never sent you that.
The Complainant: Was it one of your four friends then?
Brady: Oh you mean a long, oh you mean years ago?
The Complainant: Yeah
Brady: I didn't send that to you, but yes that was sent to you. [unclear]
The Complainant: No but I was trying to find it.
Brady: Mmm I would've figured you would've deleted it long ago

The Complainant: Well yeah, but I was like ohh

Brady acknowledges the timeframe in which he and the Complainant were involved with each other:

The Complainant: Your journal?
Brady: Uh huh, I journaled everyday in the hospital about what took place between well the last part of December 2015 and mmm I guess up until July when I left.

Brady and the Complainant discuss doing sexual things together via video chat:

The Complainant: Wait I have asked this before already? I feel like I probably did. Like you didn't...like I don't know how to say it. You didn't like jerk off to me right? Like the videos or whatever or did you? Was that like part of it?
Brady: You broke up
The Complainant: Oh...you didn't like save the videos of me doing whatever and then jerk off to them later right?
Brady: No
The Complainant: No, that wasn't that wasn't your thing?
Brady: No. There where times that you and I would just do stuff. You know. There was that, but that was entirely different.
The Complainant: Wait, what do you mean?
Brady: I mean there were times you would do stuff with me. That was not recorded.
The Complainant: Oh like just normal, Skype calling?
Brady: Sexual, yeah. But it was just you and I. There was the occasional FaceTime in addition to Skype.
The Complainant: Hm, all I remember is like super late night, hairbrush up the ass type of stuff.
Brady: What the fuck [laughing] I think you cringe just saying that too.
The Complainant: But like I have a very specific memory of that.
Brady: Oh my gosh [says the Complainant's name]
The Complainant: Sorry it's just so weird talking to you my brain is kind of scattered.
Brady: No it's fine, I'm just like wow.
The Complainant: What do you mean wow.
Brady: The way you just said it, super late night hairbrush up the ass kinda stuff.
The Complainant: I mean its not...
Brady: And you turn and you turn away and try to hide your face
The Complainant: I'm not wrong am I?
Brady: No

Brady continued the conversation noting the abuse and harm he caused to the Complainant, stated that certain things were outside of his control.

Brady and the Complainant discuss how the Complainant now has slight masochistic tendencies stemming from the abuse:

> **Brady:** Liking it doesn't make you a bad person, although I'm not bringing neck ties to get coffee, so you don't have to deal with that.
> **The Complainant:** Thanks
> **Brady:** Mmhmm. Unfortunately I left the paddle whip in Pittsburgh, so thats [unclear] too.
> **The Complainant:** How unfortunate you'll have to improvise.
> **Brady:** You'll have to swing by like [unclear], you'd have to get some needles.
> **The Complainant:** Never, that is not something
> **Brady:** I'll just swing by Staples and get a couple binder clips
> **The Complainant:** Oh I forgot about that.
> **Brady:** That I was okay with. The needles [unclear].
> **The Complainant:** You were okay with the needles?
> **Brady:** No I was okay with the binder clips
> **The Complainant:** Binder clips hurt though, they hurt more than the needles. I hated keeping the needles in too.

32. Based on your affiant's training and experience, those who engage in extortion often have multiple victims. Additionally, most individuals involved in child pornography and child exploitation matters, store their media in various places to include, internal and external hard drives, thumb drives, memory cards desktop computers, laptop computers, mobile devices, and cloud storage.

33. As noted in paragraphs 27 and 28, subpoenas were served to Snapchat for the username "TheRealBoris7", which Brady used to communicate with the Complainant. The results yielded an IP address which was ultimately assigned to the SUBJECT PREMISES. On September 12, 2019, Brady was arrested by Chesterfield Police Department for bribery. On September 25, 2019, a judge issued a bond for Brady, which included ankle monitoring, amongst other restrictions. Since then, the Chesterfield Police Department has consistently monitored the ankle device. As of January 22nd, 2020, Brady was residing at the SUBJECT PREMISES.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

34. As described above and in Attachment B, this application seeks permission to search the SUBJECT PREMISES for evidence of violations of 18 U.S.C. §2422(b), §2251, and §2252A, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

35. Based on my training and experience, I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve as both an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. I submit that if a computer or other electronic device or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe that evidence of violations of 18 U.S.C. §2422(b), §2251, and §2252A, will be stored on such devices device, for the following reasons:

Digital Evidence

a. Deleted files, or remnants of deleted files, may reside in free space or slack space for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

b. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that

show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

c. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered by using forensic tools, months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

d. Computer storage media, such as internal hard drives, contain electronic evidence of computer usage. This forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not delete this evidence because special software is -usually required for that task.

e. Information stored within a computer and other electronic storage media may provide crucial evidence of user attribution In my training and experience, information stored within a computer or storage media (e.g., registry information,

communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed.. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed .For example, computers typically contain information that logs computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera).

Forensic Analysis

36. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement

laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it is impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear as though the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

37. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often instrumentalities of a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that

they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may serve as instrumentalities of a crime. For example, they not only serve as the instrument through which the perpetrator of the Internet-based crime connected to the Internet, they also may contain logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

38. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize physical and forensic analysis of such media ,consistent with the warrant.

SPECIFICITY OF SEARCH WARRANT RETURN AND NOTICE REGARDING INITIATION OF FORENSIC EXAMINATION

39. Consistent with the Court's current policy, the search warrant return will list the model(s) and serial number(s) of the seized DEVICES. Moreover, the Government will file a written pleading in this case within one hundred twenty (120) days after the execution of the search warrant notifying the court that the imaging process of digital evidence seized from the target location is complete, and the forensic analysis of computers and media has begun. Such notice will include confirmation that written notice has been provided to the defendant or defendant's counsel informing the defendant that the forensic examination of evidence seized from him has actually begun. Such notice to the defendant and the Court is not intended to mean, and

should not be construed to mean, that the forensic analysis is complete, or that a written report detailing the results of the examination to date will be filed with the Court or provided to the defendant or defendant's counsel. This notice does not create, and is not meant to create, additional discovery rights for the defendant. Rather, the sole purpose of this notice is to notify the defendant that, beyond the simple seizure of his property, a forensic search of that property has actually begun.

BIOMETRIC ACCESS TO DEVICES

40. This warrant permits law enforcement to compel "Brady" to unlock any DEVICES requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

41. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

42. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button)

located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

43. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

44. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

45. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

46. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the DEVICES subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.

47. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

48. Due to the foregoing, if law enforcement personnel encounter any DEVICES that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of Brady to the fingerprint scanner of the DEVICES found at the PREMISES; (2) hold the DEVICES found at the PREMISES in front of the face of Brady and activate the facial recognition feature; and/or (3) hold the DEVICES found at the PREMISES in front of the face of Brady and activate the iris recognition feature, for the purpose of attempting to unlock the DEVICES in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to request that Brady state or otherwise provide the

password or any other means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize law enforcement to ask Brady to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

CONCLUSION

49. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located at the SUBJECT PREMISES, described in Attachment A. I respectfully request that this Court issue a search warrant for the SUBJECT PREMISES authorizing the seizure and search of the items described in Attachment B.

Respectfully submitted,

Christopher A. Ford
Special Agent, FBI

SEEN

Alexandra Williams
Special Assistant U.S. Attorney

Subscribed and sworn to before me on 2/12/2020.

/s/
Roderick C. Young
United States Magistrate Judge
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

The SUBJECT PREMISES at **19820 OAK RIVER DR, PETERSBURG, VA 23802** is described as a one story single family home with a possible basement. The front door is red with beige in color paneling. The house has red shutters and wood steps going up to the front door. The driveway is dirt and is not paved. The black mailbox on the street has the number "19820" affixed to it. There is a white RV in the driveway. Behind the house appears to be a shed.

ATTACHMENT B

Specific Items to be seized

Any and all devices or records located at the subject premises as described in Attachment A and found to have been utilized by Joshua Brady, including but not limited to :

c.) Any DEVICE (defined below) capable of being used as a means to commit the violations described above or on which any aforementioned items can be stored, secreted, saved, edited, or transmitted, to include cellular telephones, cameras, handheld devices (such as iPods, iPads, or similar devices), computers, hard drives, flash drives, CDs, DVDs, SIM cards or memory cards.

d.) Records and information relating to the production, distribution, receipt, or possession of visual depictions of minors engaged in sexually explicit conduct, including any visual depictions of children such as child pornography (as defined in 18 U.S.C. § 2256) and child erotica, and any records which may assist in the identification of those children.

e.) Photographs of the inside of the residence and items contained therein in order to identify the location and identities of individuals depicted in images and videos of child pornography.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of DEVICE or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "DEVICE" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.